Stasis Trap: Cross- Layer attack & its Defense in Cognitive Radio Networks

By

DILEEP NAGIREDDYGARI

Bachelor of Technology in Information Technology

Vellore Institute of Technology University

Vellore, TN, India

2010

Submitted to the Faculty of the Graduate College of the
Oklahoma State University in partial fulfillment of the
requirements for the Degree of
MASTER OF SCIENCE
May 2014

Stasis Trap: Cross- Layer attack & its Defense in Cognitive Radio Networks

Thesis proposal approved:

Dr. Johnson Thomas

Thesis Adviser

Dr. Subhash Kak

Dr. David Cline

Name: DILEEP NAGIREDDYGARI

Date of Degree: MAY, 2014

Title of Study: STASIS TRAP: CROSS LAYER ATTACK & ITS DEFENSE IN COGNITIVE RADIO NETWORKS

Major Field: COMPUTER SCIENCE

ABSTRACT: Spectrum shortage is a major problem in wireless communications. Existing research on attacks and security issues in CR networks focus on individual network layers. In this thesis, we identify a cross-layer attack, called the Stasis Trap attack. This attack is launched from the MAC layer as the point of attack but the final target goal is to degrade TCP layer end to end throughput of flows by exploiting the TCP congestion control mechanism in cognitive radio. The chances of the attacker being detected are low owing to the fact that the target layer is different from the layer where the attack is launched.

An adversary launches an attack on the MAC layer causing large variations in Round Trip Time (RTT) resulting in a large drop in throughput of TCP flows (drop of around 40% from our simulation results) but has little effect on the MAC-layer throughput and hence is very difficult to detect.

A defense for this Stasis Trap attack is proposed using a deterministic key pre-distribution algorithm where the keys are pre-distributed to nodes and If any two nodes want to communicate with each other, they either search for a common key and a common channel between them or look for intermediate nodes which have the same in common and communicate through them. Simulation results show that the throughput was restored to its original levels using key pre-distribution.

Table of Contents

Chapter Page

I. INTRODUCTION **1**

1.1 Overview of Cognitive Radio Networks 1

1.2 Problem Statement 2

1.3 Research Objective 3

1.4 Organization of Thesis 4

II. REVIEW OF RELATED LITERATURE **5**

2.1 Cognitive Radio Networks 5

2.2 Distributed Channel Negotiation in MAC Layer 9

2.3 Conventional Detection Technique 10

2.4 Transport Layer Protocol 11

2.5 Individual Layer attacks in Cognitive Radio Network 14

2.6 Chinese Remainder Theorem 19

2.7 Routing Schema in CR Network 20

III. STASIS TRAP ATTACK IN CR NETWORKS 23

3.1 Overview of Stasis Trap Attack 23

3.2 Algorithm 26

3.3 Simulation Results 28

3.4 Conclusion 32

IV. DEFENSE BASED ON KEY PRE DISTRIBUTION 33

4.1 Overview 33

4.2 Key Pre Distribution Phase 34

4.3 Key Pre Distribution in CR Network 39

4.4 Algorithm 46

4.5 Simulation Results 48

V. CONCLUSION 56

REFERENCES 57

LIST OF TABLES

Page

Table 1: Key Chains distributed to each node 38
Table 2: Generating Keys for the above example.....42
Table 3: Node-Id with their keys and common keys 54

LIST OF FIGURES

Page

Figure 1: Cognitive Radio Architecture....7
Figure 2: Distributed Channel negotiation process....9
Figure 3: Qualified Observers....11
Figure 4: Network Layout in CR networks....12
Figure 5: Transport Layer interface for CR networks....13
Figure 6: Alternating phases in Cognitive Radio MAC....18
Figure 7: Routing Schemes in CR Network....21
Figure 8: Layered Graph Schema....22
Figure 9: Stasis Trap Attack Scenario....24
Figure 10: Pictorial representation of Stasis Trap Attack....27
Figure 11: Layout of CRN consists of 50 nodes....29
Figure 12: Throughput Analysis before attack vs Time....30
Figure 13: Throughput Analysis after attack vs Time....31
Figure 14: Throughput Analysis before & after attack vs Time....31
Figure 15: Common Channel list in CR Nodes....43
Figure 16: N1 wants to communicate with N6 which don't have a common channel....44
Figure 17: Pictorial representation for communication between source and destination....47
Figure 18: Key Connectivity with different set of PRP numbers....50
Figure 19: Key Connectivity for various network sizes with constant keychain size....51
Figure 20: Key Connectivity for various network sizes with different keychain sizes....52
Figure 21: An alternative path when an intermediate node of TCP flow is attacked....54
Figure 22: Throughput Analysis vs Time after applying Key pre distribution Algorithm 55

CHAPTER I

INTRODUCTION

1.1 Overview of Cognitive Radio Networks

Cognitive Radio (CR) Networks aim to make good use of vacant spectrum. This technology allows the coexistence and sharing of licensed spectrum resources between two types of users, licensed (Primary Users or PU) and unlicensed (Secondary Users or SU). This helps to solve the problem of spectrum sharing by allowing SUs to use primary systems without interference. CR nodes can sense their environment and spectrum, `analyze the discovered information, and adjust to the sensed environment.

Cognitive Radio techniques provide the capability to use or share the spectrum in an opportunistic manner [3]. CR:

- ➢ Enables the users to determine which portions of the spectrum are available and detect the presence of Primary Users (Spectrum Sensing).
- ➢ Selects the best available channel (Spectrum Management).
- ➢ Coordinates access to this channel with other users (Spectrum Sharing).
- ➢ Vacates the channel when a licensed user is detected (Spectrum Mobility).

IEEE 802.11 MAC protocol's Distributed Coordination Function (DCF) is effective in coordinating channel access for contending nodes. However, it is a completely different

case in a hostile environment as, DCF is vulnerable to attacks. This results in exploiting the contention coordination mechanism against the MAC protocol which can range from selfish exploitation to malicious network disruptions [8].

In Cognitive Radio, we need to firstly identify (i) requirements of protocols for the transport layer of Cognitive Radio networks. (ii) propose a generic architecture for implementing the protocols. (iii) design, implement and evaluate the best-effort transport protocols [2]. The protocols proposed can use information from all layers and estimate parameters to provide efficient services to the applications.

The launch of multiple-layer attacks where there may be some coordination of attack activities between different layers is more pronounced in CR technology [6]. Attackers have the capability to launch attacks in multiple layers simultaneously. In this paper, we show how attackers can significantly reduce throughput whilst being undetected. Here we choose Stasis Strap attack (cross layer attack) where the target layer is different from the point of attack, thus making the attack stealthy.

1.2 Problem Statement

In this paper, we identify a cross-layer attack called “Stasis Trap” attack that can be launched in CR networks. In this attack, the adversary uses the MAC layer as point of attack and ultimately aims to degrade TCP layer throughput of flows within its transmission range [1]. In CR networks, unused spectrum bands are recognized and data

is gathered, using distributed spectrum sensing. The information collected is used by the dynamic spectrum allocation mechanism. MAC protocols use the common control channel which plays an important role in enabling the nodes to exchange local information. There is a channel contention problem, where Distributed Coordination Function adopts a back-off mechanism, by manipulating the back-off value by using a small contention window [4]. The adversaries transmit data for a certain amount of time to cause delays in the TCP flows that are traversing through neighboring nodes, and then stop the transmission. This process of preempting the channel is repeated after a certain time duration.

Though the transport protocols are planned to provide reliable end-to-end transport service, due to the periodic blocking of the channel due to the stasis trap attack, there are periodic delay spikes in the TCP flow. This would result in Retransmission Timeout (RTO). Due to this the, the congestion control mechanism reduces the congestion window size to one and the outstanding packets are re-sent.

1.3 Research Objective

Though a considerable amount of research has been done on the susceptibilities of the CR network layers, very little investigation regarding cross-layer attacks has been done. These attacks are difficult to detect mainly because of the way they attack the network. They make use of the liabilities of a specific layer (attack point) and end up disrupting the

functioning of another layer (target layer). They are difficult to detect because the attack and target points belong to different layers.

Our goal is to design a cross-layer attack called ‘Stasis Trap’ in Cognitive Radio Networks where the point of attack is at the MAC layer and aims to degrade TCP layer (target layer) throughput by exploiting TCP’s congestion control mechanism. We design a defense for this attack by using a novel key pre distribution scheme which uses the Chinese remainder theorem for generating keys [11].

1.4 Organization of Thesis

The remainder of this thesis document is organized as follows. In Section II we briefly review the Related Work of MACs DCF and Transport Layer Protocol with its rules. In Section III we go through the Stasis Trap attack in CR network and in Section IV we provide a defense for this attack based on key pre-distribution using the Chinese remainder theorem.

CHAPTER II

REVIEW OF RELATED LITERATURE

The following sections give an overview of Cognitive Radio networks and explain its functionalities in the MAC layer and Transport layer. We focus on the attacks at these layers. Next we look at the Chinese remainder theorem and routing schema in CR which we used for defense against this attack.

2.1 Cognitive Radio Networks

Cognitive Radios are expected to mitigate the spectrum scarcity problem through intelligent use of the fallow spectrum bands. However, as CRNs are wireless in nature, they face common security threats found in traditional wireless networks. Current literature on CRNs describes several approaches for spectrum sensing, spectrum management and spectrum mobility which may face new security threats and challenges. CR has two main characteristics [3]

- **Cognitive capability**: makes the devices capable of sensing their environment and choosing the best available transmission mode in the free spectrum bands. This becomes feasible through the spectrum management process where several physical layer parameters are estimated.
- **Reconfigurability**: this enables a CR to change several of its parameters and adapt to its environment. This is very important because if any PU transmission is detected,

the CR should vacate the band.

Since most of the spectrum is already assigned, the most important challenge is to share the licensed spectrum without interfering with the transmission of other licensed users. The temporarily unused spectrum is referred as ‘spectrum hole or whitespace’ which is used by the unlicensed users (Secondary users).

Cognitive Radio Architecture

The CRN architecture is classified into two groups, the primary network and xG network (Cognitive Network) [3].

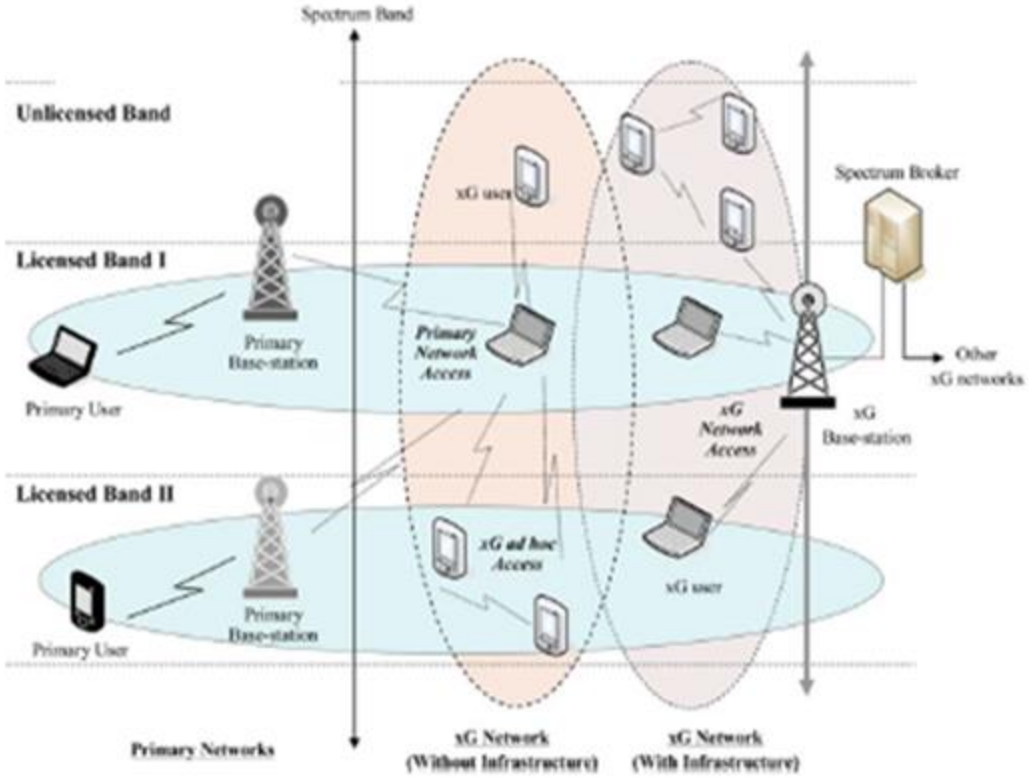

Figure 1: Cognitive Network Architecture [3]

Primary network: An existing network is referred as the primary network, which has exclusive right to a spectrum band.

- **Primary User or PU (Licensed user)** has a license to operate in a designated spectrum band. This access can only be controlled by the primary base-station.
- **Primary Base-station:** It is a fixed infrastructure network component which has a spectrum license. The primary base station does not have any cognitive capability for spectrum sharing with cognitive users.

Cognitive Network: Cognitive Networks do not have license to operate in the desired band and hence, they use the different Cognitive Radio techniques which provide the capability to use or share the spectrum in an opportunistic manner.

- **Cognitive (xG) user (Secondary User):** This user has no spectrum license. Hence, it requires additional functionalities to share the licensed spectrum band.
- **Cognitive (xG) base-station:** The Cognitive users connect to a Cognitive base-station which provides a single-hop connection to them without spectrum access license. A cognitive user can accesses other networks, through this connection.
- **Spectrum broker:** The spectrum broker is a central network entity that plays a role in sharing the spectrum resources among different cognitive networks. The broker is connected to each network and can serve as a spectrum information manager to enable coexistence of multiple cognitive networks.

Cognitive users can communicate with each other in a multi hop manner or access the base station.

Cognitive (xG) network access: Cognitive users can access their own base-station both on licensed and unlicensed spectrum bands.

Cognitive (xG) ad hoc access: Cognitive users can communicate with other cognitive users through ad hoc connection on both the bands.

Primary network access: The cognitive user can also access the primary base-station

through the licensed band.

2.2 Distributed Channel Negotiation in MAC layer

In CR networks channel negotiation is carried in a distributed manner, between sender and receiver. During channel negotiation, MAC frames are used as: *Free Channel List (FCL), SELection (SEL), and REServation (RES) [4]*.

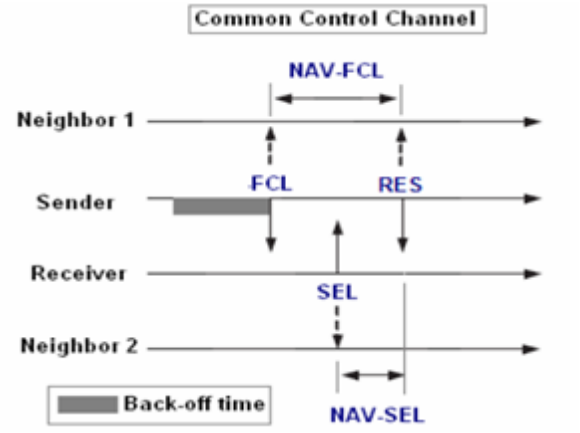

Figure 2: Distributed Channel negotiation process [4]

Initially, the sender identifies fallow spectrum bands and allots them into logical channels, to obtain FCL and sends it to the receiver after a back-off time. After receiving the FCL, the receiver identifies available channels common to both sides and chooses one data channel by indicating SEL frame and the sender notifies its neighbors of the channel selection with a RES frame. When the sender transmits FCL frame, the Neighbor 1 refrains from transmitting, by maintaining a network allocation vector (NAV) specified in the FCL and SEL frames overhead during the channel negotiation process.

In order to avoid RTS collision, the node that is to transmit the data needs to delay the transmission for a back-off period. The back-off value is selected arbitrarily from the range [0, CW] (where CW – contention window size). . A node transmits RTS frame to reserve a channel when the back-off value is reduced to zero. If an adversary uses a small CW value, it can preempt the channel and prevent others from accessing it.

2.3 Conventional Detection Technique

To detect such misbehaviors, a sequential analysis is performed whilst observing the back-off value to detect these types of attacks. The nodes that are within the transmission range can measure the back-off value.

A Sender with data to transmit has to defer transmission for a back-off period to avoid an RTS collision. The back-off value is chosen from the range [0, CW] where CW is the contention window size. When the back-off timer is decremented to zero, then the sender can send frames to reserve the channel. If the attacker uses a small CW value, it can preempt the channel and prevent others from accessing the channel with a high probability [2].

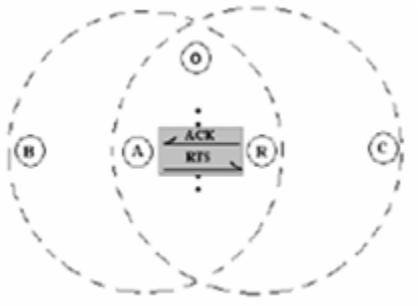

Figure 3: Qualified Observers [1]

In the above figure 3, node A is an attacker. Node A transmits data to node R. In this scenario, node R and O can calculate the back-off time value by computing the time interval between the ACK transmitted from R. The term qualified observers is used to describe the nodes that are located within the transmission range of both MAC sender and receiver, which are qualified to calculate the back-off times used by the sender. We specify R and O as qualified observers.

However, the adversary could escape from detection by changing its transmission destination. In the above situation node A transmits to R for some time and periodically changes its direction to node B before the qualified observers spot the intruder. Using this technique, the attacker can thwart detection of sequential tests performed by neighboring nodes.

2.4 Transport Layer Protocol

The Network layout for standard TCP protocol in CR networks is as below.

Figure 4: Network Layout in CR Networks [2]

The above layout of the TCP network is used for simulation purposes. The router represents a gateway. The connection between router and destination is wired or wireless. The link between source and router will be changed based on the whether the primary user is present or not. The CR-link alternates between spectrum sensing and transmission modes. This shows periodic abrupt increase or decrease of RTT (round trip time) [2]. When CR-link changes to spectrum sensing mode, no packets are received by the source. After the completion of spectrum sensing the source node receives several acknowledgments which were waiting in network and thus the RTT is then calculated. This is the reason there is an abrupt increase in RTT.

If the spectrum sensing duration combined with the currently observed RTT is greater than RTO (Retransmission Time Out) timer value, then RTO timer expires while the CR node is in the spectrum sensing state. Timeouts, closing the congestion window are reduced to half of the previous size and the TCP gets into slow-start state.

The cognitive Transport layer is shown in the below diagram and its interfaces with the upper and lower layers.

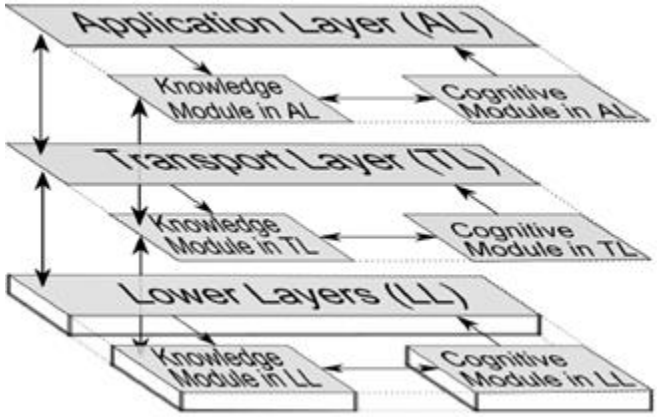

Figure 5: Transport Layer Interface for Cognitive Networks [2]

The cognitive functionality in the transport layer is divided into two modules; the Knowledge module (KM) which is for storing information or knowledge about the application's need and the status of local and global networks; the Cognitive module (CM) is for algorithms and heuristics for gathering knowledge and to control signals with the KM [2].

Decision Making Rules of the transport layer protocol in CR networks are [2]:

- R1: If estimate of cwnd (congestion window) is known, then
    i. Set cwnd to the estimated cwnd and
    ii. Enter into the congestion-avoidance state
- R2: If $rtt[i] > rtt[i-1] + 0.9 \times ssd$, Then the packet is delayed because of spectrum sensing (*rtt* – Round Trip Time, *ssd* – Spectrum Sensing Duration, *i* - index of the packet).

- R3: If packet delayed because of spectrum sensing, and then they do not update *rtt* or *srtt*
- R4: If RTO timer expires while sensing spectrum then reset RTO timer and take no further action (RTO – Retransmission Timeout).
- R5: If BW_C decreases then set cwnd to match BW_C. (BW_C – Available bandwidth)
- R6: If BW_C increases and $EBW_I \geq BW_C$ then set cwnd to match BW_C. (EBW_I – Estimated Bandwidth)
- R7: If BW_C increases and $EBW_I < BW_C$ then
    i. Set cwnd to match EBW_I AND
    ii. Enter slow-start state

2.5 Individual Layer attacks in Cognitive Radio Network

Based on the layer, attacks have been classified into Physical, Link, Network and Transport. Ad Hoc attacks can target Cognitive Radio (CR) networks which are also considered to be Ad Hoc networks [7].

Physical Layer Attacks

Primary User Emulation (PUE): According to the CR model, a Secondary user (SU) is allowed to use a specific band as long as it is not occupied by any Primary User (PU). When it detects the presence of a PU, it switches channels immediately to an alternative band. If a SU is detected, then they both share the same band using certain mechanisms

that are used to share the spectrum fairly.

However, a malicious secondary user may emulate a primary user to obtain the resources of the channel so that it does not have to share the same band with the other secondary user. This is called a PUE attack [7].

Objective Function Attack: Cognitive Radio has the ability to sense the external environment, learn from the history and make intelligent decisions to adjust its transmission parameters. The 'Cognitive Engine' is used to find the radio parameters appropriate to the current environment.

An attacker can launch this attack by manipulating the parameters (transmission rate) to make the results biased to his interest [7].

Jamming: An attacker (Jammer) may send continuous packets of data making a legitimate user to never sense a channel as idle or may force them to receive junk packets. The most dangerous attack would be to jam the dedicated channel that is used for spectrum sensing information between CRs [7].

Link Layer Attacks

Spectrum Sensing Data Falsification: In this type of attack, an attacker sends false local spectrum sensing results to its neighbors, causing the receiver to make a wrong spectrum-sensing decisions [7].

Control Channel Saturation DOS Attack: In multi-hop CRN, CRs communicate with each other after performing a channel negotiation process in a distributed manner. During this phase, MAC control frames are exchanged to reserve the channel. An attacker can utilize this feature to decrease the network performance by forging the MAC control frames for the purpose of saturating the control channel [7].

Selfish Channel Negotiation: In multi-hop CRN, a CR host can refuse to forward any data for other hosts. This will allow it conserve its energy and increase its own throughput [7].

Network Layer Attacks

Sinkhole Attack: An attacker advertises itself as the best route to a specific destination, luring neighboring nodes to use it to forward their packets [7].

HELLO Flood Attack: An attacker sends a broadcast message to all the nodes in a network with enough power to convince them that it is their neighbor. However, their packets will be lost and if anode discovers the attack it will be left with no neighbors to forward its packets because all of them would be using the same route [7].

Cross Layer Attacks in Cognitive Radio Networks

Lion Attack: This attack is considered as a cross-layer attack where the point of attack is at the Physical layer (Primary User Emulation Attack) to disrupt the TCP connection in

the Transport layer. This attack will force CRN to perform frequency handoffs, thus degrading TCP performance [7].

Attack A1: Attackers can reduce channel utilization by [6]

- Making honest secondary users wrongly believe the existence of a primary user when it is absent through PUE attack or Reporting False Sensing Data Attack (RFSD) in Physical Layer.
- Reducing the probability of honest secondary users utilizing the channel in MAC layer, through common control channel DoS attack, Small back-off window attack (SBW).

These attacks have an "OR" Relationship, one attack can achieve the goal of reducing the channel utilization.

Attack A2: When CR node is near to the PU while it is transmitting, they cause interference to the primary user [6].

- CR nodes fail to detect the existence of the primary user, which can be done through RFSD (Reporting False Sensing Data) attack.
- They have to transmit data and this can be achieved through routing protocols in the network layer.

Here the attack in Physical layer and network layer have an "AND" relationship.

Distortion of Spectrum Availability

CR MAC protocols rely on cooperative sensing mechanisms to determine the set of free channels. A malicious CR can report false sensing observations to distort the spectrum availability. A single false report can prevent access to idle channels [7] [9].

Spectrum distortion can be easily achieved in spectrum information sharing techniques that utilize the spectrum using busy tones. These tones are unauthenticated and they can be transmitted by any CR without reflecting the true channel state.

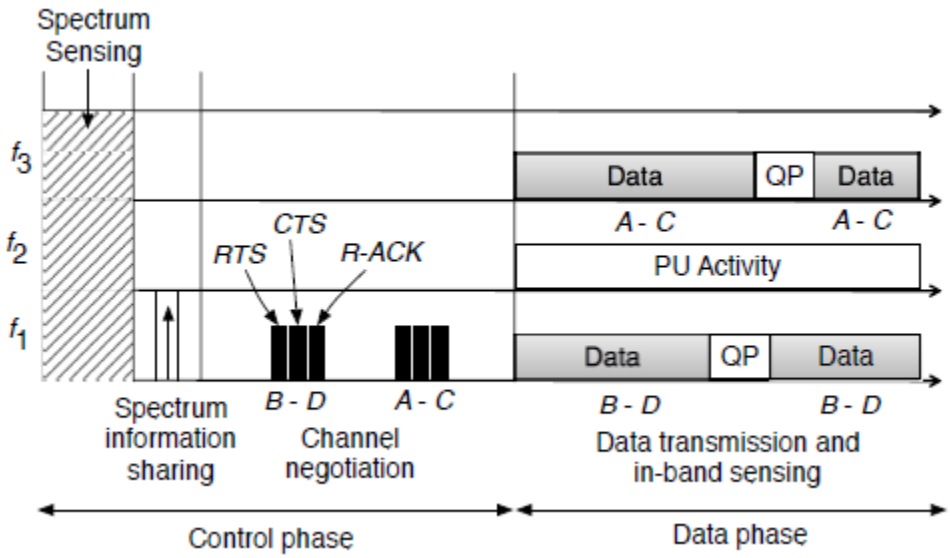

Figure 6: Alternating phases in Cognitive Radio MAC [5]

In the above diagram, there are four CRs A-D and three channels f_1-f_3. During spectrum sensing phase, CRs A-D determines that f_2 is occupied by PU. In the spectrum

information sharing phase, CRs transmit a busy tone to indicate that f_2 is occupied. This is the Alternating control and data phases for a CR- MAC [5].

During the control phase, CR sense for the idle channels and share their sensing observations by transmitting busy tones on dedicated time slots. Cognitive Radios negotiate the spectrum allocation for the upcoming data phase. During the Data phase, CRs switch to the negotiated channels. To avoid interference In-band sensing is performed with Primary users. A PU may appear at any channel during the data phase, thereby incorporating a periodic quiet period (QP) during which CRs perform in-band sensing. If a PU is detected, CRs abandon the current channel by switching to a back-up one.

For example, a malicious Cognitive Radio D could transmit a busy tone on every slot during the spectrum information sharing phase, thus indicating that channels f_1-f_3 are occupied by Primary Users. CRs A, B and C will differ from communicating in the upcoming data phase.

2.6 Chinese Remainder Theorem:

We proposed a defense to the Stasis Trap attack based on key pre-distribution using the Chinese Remainder theorem (CRT) [11]. Here, we are using CRT for generating keys. We chose CRT for key generation because this scheme is suitable to achieve a goal which supports large network size with a small key pool.

The Chinese remainder theorem is a result about congruence in number theory. Its basic form will determine a number 'n' that when divided by some given divisor leaves given remainders [11].

Given the moduli set m_i for i=1,2,…n such that all are relative primes, i.e., $gcd(m_1, m_2)$ = 1 for $i \neq j$, there exists a unique number 'u' in the range [$0, M-1$] where $M=m_1,m_2....m_n$ and let $r_1r_2...r_n$ be integers. Then the congruent equations $x \equiv r_1 \textbf{mod} m_1$, $x \equiv r_2 \textbf{mod} m_2$, ... $x \equiv r_n \textbf{mod} m_n$ => $x = \sum_{i=1}^{n} M_i' M_i (\textbf{mod}\ M)$ *where* $M_i = M/m_i$ *and* $M_i' = M_i^{1} (\textbf{mod}\ n_i)$.

For example, Let m_i={2,3} where m_0=2 and m_1=3, M=2*3=6, Let A be the nodes in a network. A->{0,1,2,3,4,5}. Using CRT {(A, A **mod** m_0), (A, A **mod** m_1) } the tuples generated are {(0,0),(1,1),(0,2),(1,0),(0,1)(1,2)}.

2.7 Routing Schema in Cognitive Radio Network

In order to do the distribution of the keys that were generated using the CRT, it is essential to know the routing schema of the CR network. Hence, we review the routing schemas.

For multi-hop CRN's routing is grouped into 2 categories:

- Approach based on the full spectrum knowledge
- Approach based on local spectrum knowledge.

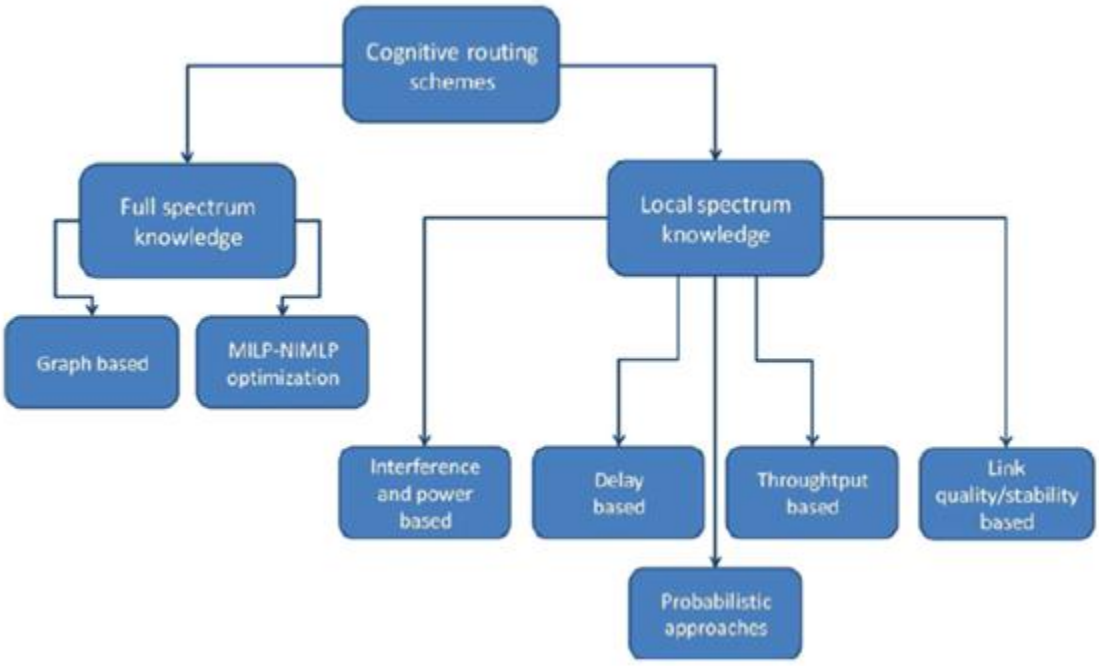

Figure 7: Routing Schemes in CR network [12]

Here, we choose the Graph based approach which needs a full Spectrum Knowledge to pre-distribute the keys in the network. In the graph based approach, a route designing is done using graph abstraction & route calculation [12].

Graph Abstraction: This refers to the generation of a logical graph representing the network topology.

Route Calculation: This generally deals with designing a path in the graph connecting source-destination pairs.

Graph based routing approach through layered-graphs:

The framework is based on the creation of layered graph which features a number of layers equal to the number of available channels. The edges of the layered graph can be of three types: **Access edges** (small dotted line in fig 8) connect each node with all the corresponding subnodes. **Horizontal edges** (dark line lying on the horizontal planes in fig 8) between pairs of subnodes belonging to the same logical layer are added to the graph. **Vertical edges** (dashed vertical edges in fig 8) connect subnodes of different layers of a single secondary device and represent the capabilities to switch from one channel to another.

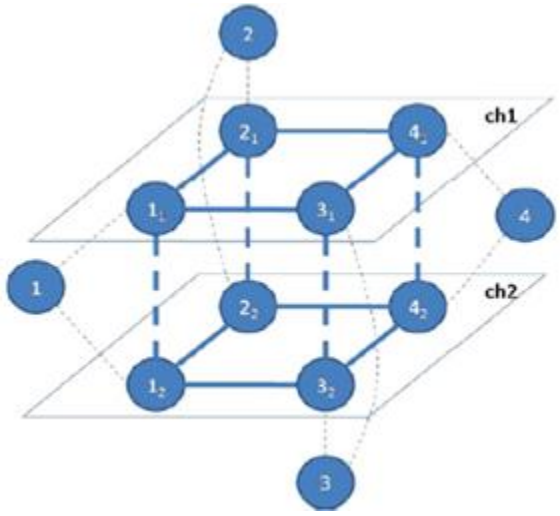

Figure 8: Layered Graph Schema [12]

CHAPTER III

STASIS TRAP ATTACK IN CR NETWORKS

3.1 Overview of Stasis Trap Attack

An attacker can manipulate MAC protocols to launch a Stasis Trap attack. This is a cross layer attack where it is difficult to detect the attacker. This Cross layer attack is launched from the MAC layer as the point of attack but ultimately aims to degrade the TCP layer's end to end throughput of flows within its transmission range by exploiting the TCP congestion control mechanism.

The stasis trap attack is launched against neighboring nodes by periodically preempting the wireless channel in order to cause large variations in Round Trip Time (RTT) of TCP flows which are within the range of the adversary. This causes a significant drop in throughput flows, thereby creating "stasis trap". It has very little effect on MAC-layer throughput and hence is very difficult to detect [1].

The adversary attacking the MAC layer can preempt the channel by manipulating the back-off mechanism. Moreover, an attacker can change the transmission destination to evade detection from qualified observers [see section 2.3]. It is difficult for a single observer to detect the attack due to the randomness of back-off values.

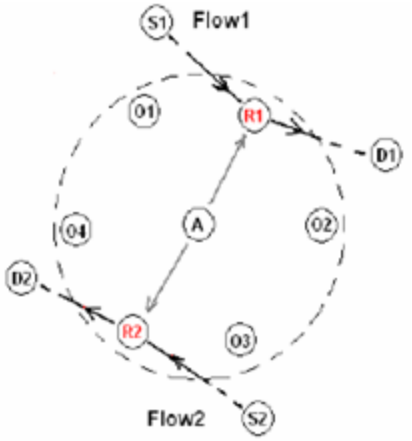

Figure 9: Stasis Trap attack scenario [1]

In Fig 9, node A is an attacker which can switch its transmission between R1 and R2 in a round robin manner. This attacker has less effect on channel contention mechanism or MAC layer throughput due to the periodic change of channel. So it gets difficult for the qualified observers [see section 2.3] to detect it. The main target of the stasis attack is the TCP layer. Its aim is to degrade the end-to-end throughput of TCP flows traversing through neighboring nodes.

In the above figure, Flow1 and Flow2 are two TCP flows. We know the RTO (Retransmission Timeout) mechanism which was designed for packet losses by calculating RTT (Round Trip Time) of the packet. If RTT is greater than RTO then the TCP sender assume there is a packet loss and responds by reducing the congestion window size and retransmitting the packet again. Now, if an attacker occupies the channel greater than RTO then the targeted flows will result in timeout. As a result the

throughput of the flows will drop significantly.

In the Transport Layer protocol, CR-link alternates between spectrum sensing and transmission modes. This CR-link shows increase or decrease variation in RTT. The reason for this is when the nodes for the CR-link enter into spectrum sensing mode, the source will not receive packets. As soon as spectrum sensing is completed the source node receives several ACK (acknowledgements) waiting in the network, which increases the RTT. Because of this waiting in the network, RTT for these packets increase by an amount equal to the spectrum sensing duration (ssd).

When CR is in sensing mode, the spectrum sensing duration (ssd) is calculated. If the RTT + spectrum sensing duration (ssd) > Retransmission Timeout (RTO), the timer expires which means the sender assumes that packet was lost and responds by reducing the congestion window size and retransmitting the packet again. As a result, the throughput of the flows will drop significantly. The congestion window sizes are reduced to half of the previous value [2], and the TCP enters into slow-start state. This happens due to the “Stasis Trap Attack” in Cognitive Radio Networks where the point of attack is at the MAC layer but the target layer is TCP layer, which degrades the end-end throughput of TCP flows.

3.2 Algorithm for Statis Trap Attack

The algorithm for Stasis Trap Attack is explained below based on fig 9.

- Step 1: S1 sends a packet to D1 through intermediate node R1 i.e. the Transport Layer flow (Flow1).
- Step 2: Attacker node A starts blocking the channel towards R1 through MAC layer at periodic intervals.
- Step 3: R1 changes to spectrum sensing mode.
- Step 4: When A diverts to the other node (R2), then R1 sends ACK to sender S1.
- Step 5: At S1, If [RTT + spectrum sensing duration (ssd) > RTO].
- Step 6: then there is a decrease in throughput.
- Step 7: else Goto Step 1.

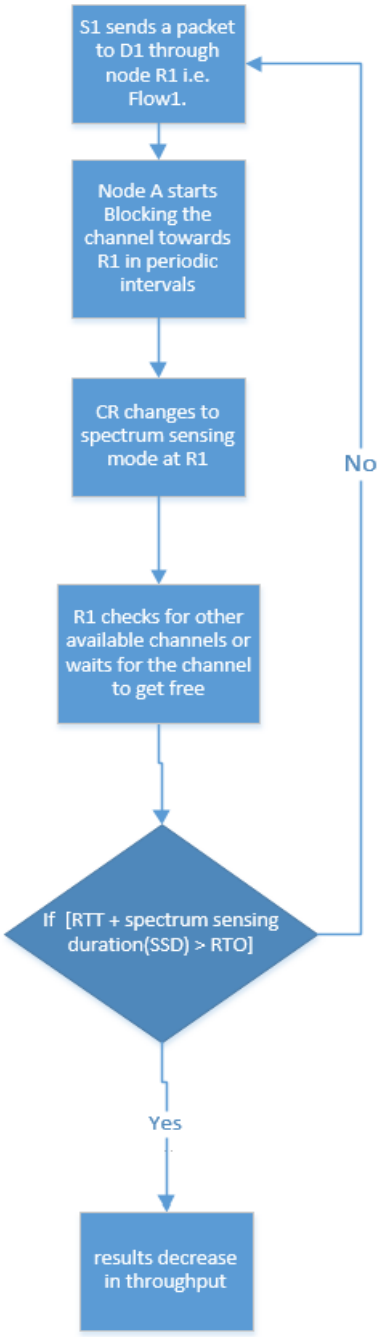

Figure 10: Pictorial representation of Stasis Trap Attack

3.3 Simulation Results

The main target of the stasis trap attack is to degrade the TCP flow and as a result throughput is reduced and network performance is degraded. Our simulation results showed that the network performance (throughput) fell down below 40%; so it is necessary for the network to be resilient to such kind of attacks.

Our simulation uses ns2.34 [15] (network simulator) to investigate the effect of stasis trap attack on network performance. Node mobility was not considered in the simulation. The network topology consists of 50 nodes. The nodes are placed randomly with equal communication range (150 meters). The source node 20 communicates with the destination node 45 through the intermediate nodes 21, 22, 23, 24. And another source node 32 communicates with destination 47 through 33, 34, 35,36. The paths are chosen based on the algorithm which calculates the shortest path between two nodes.

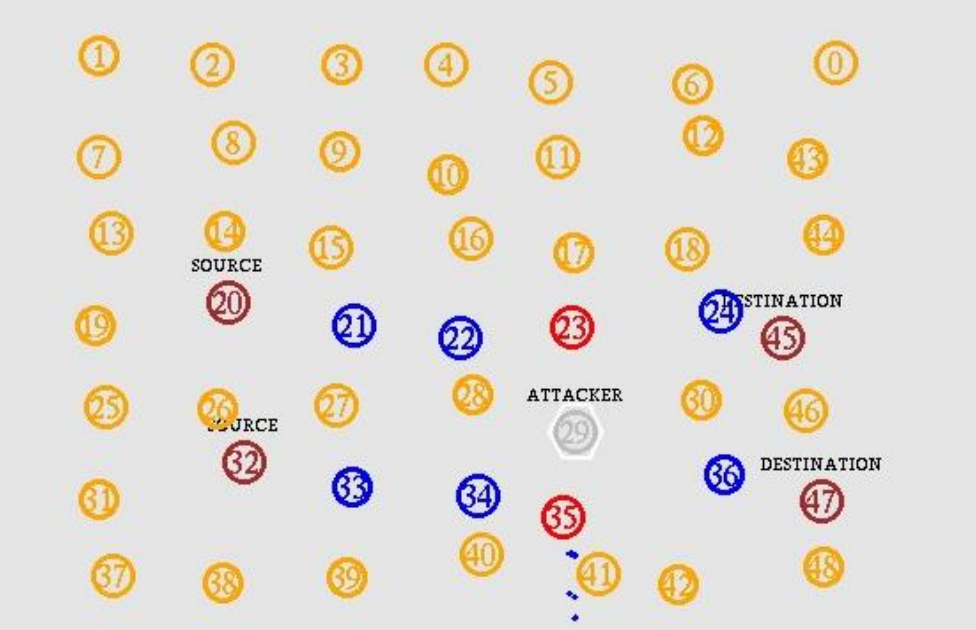

Figure 11: Layout of cognitive radio network of 50 nodes

Before transmitting data, the source nodes sends RTS message to destination i.e., REQUEST TO SEND for estimating ROUND TRIP TIME (RTT) for transmitting data to destination. After receiving RTS message from source, destination replies with CTS (CLEAR TO SEND) message. After receiving CTS message from destination, the source node starts transmitting data to destination through the intermediate nodes. At a certain time, one of the neighbors, say node-29 behaves as a malicious node and attacks the MAC layer of the intermediate nodes 23 and 35 (see figure 10). As a result the TCP FLOW is reduced and intermediate nodes 23 and 35 not able to transmit data in a constraint data rate. This is because the RTT (ROUND TRIP TIME) exceeds the RTO (RETRANSMISSION TIME-OUT) and the throughput of TCP flow decreases almost

immediately.

Simulation results show that:

- The throughput rate before cross layer attack – 97 kb/s
- The throughput rate after cross layer attack – 33 kb/s

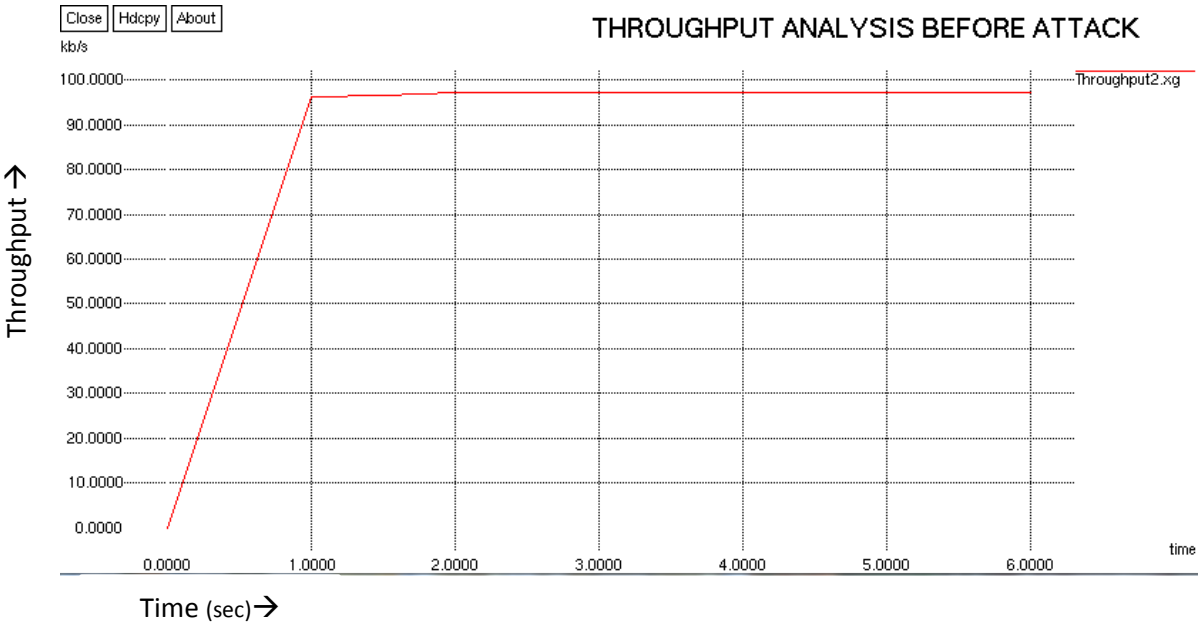

Figure 12: Throughput Analysis before Attack vs Time

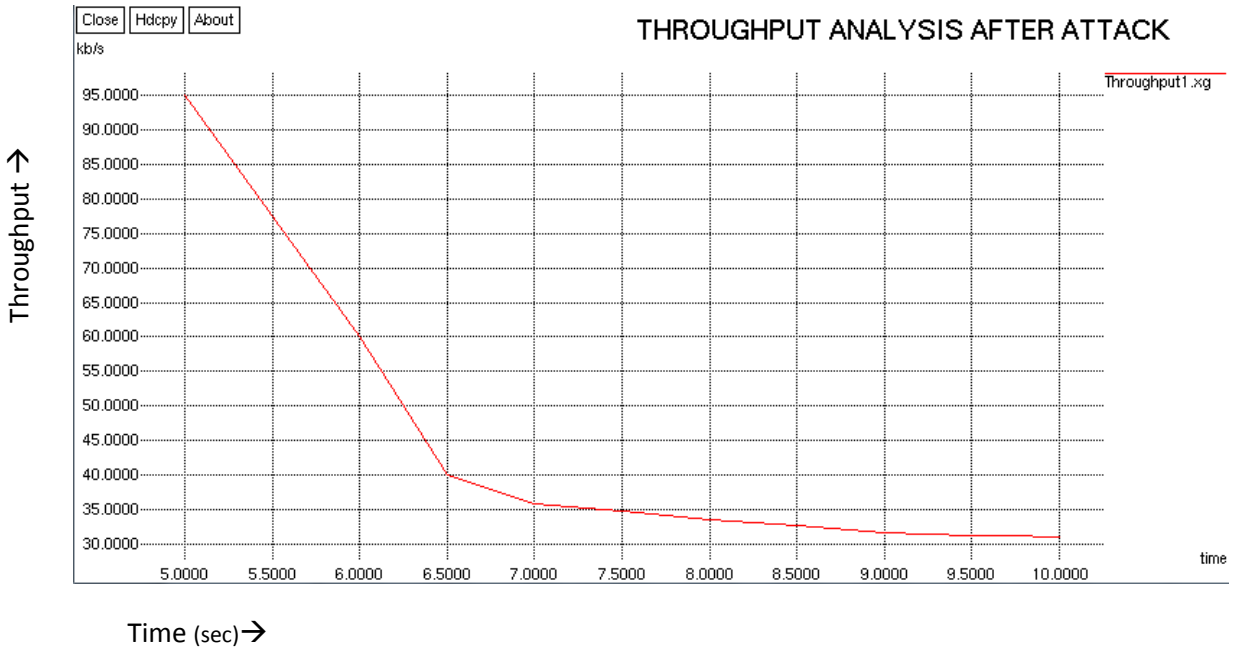

Figure 13: Throughput Analysis after Attack vs Time

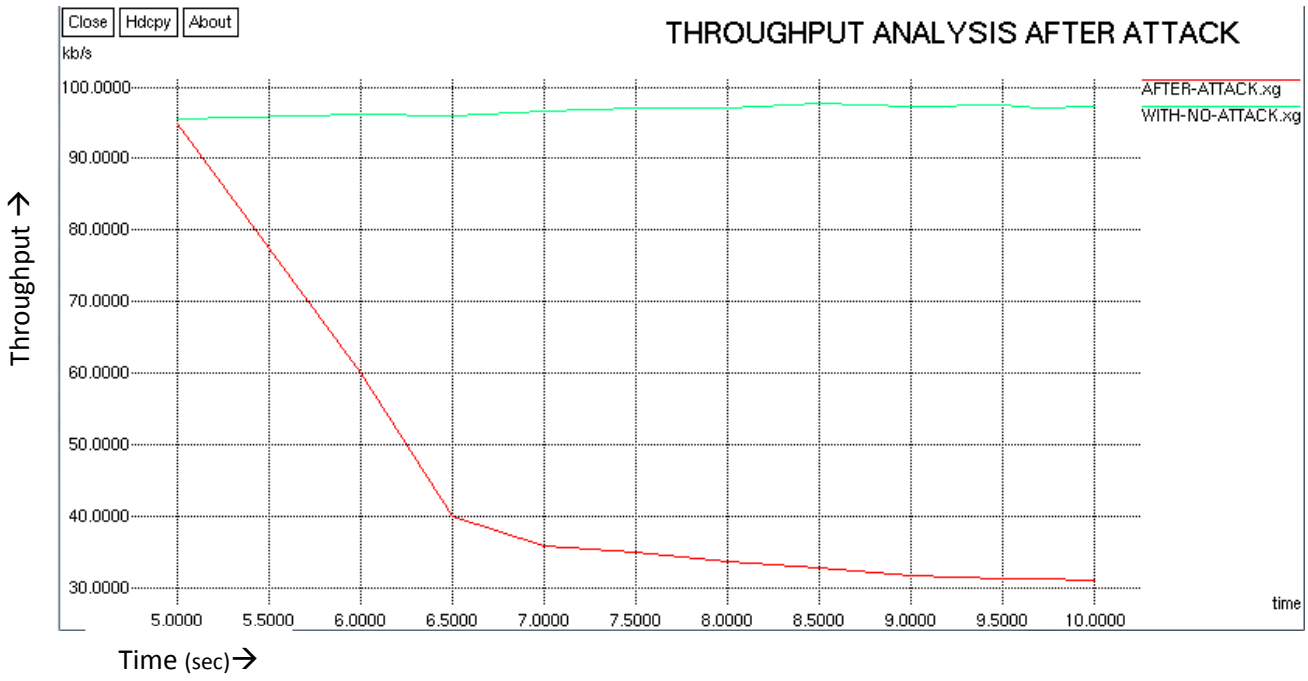

Figure 14: Throughput Analysis before and after Attack vs Time

The throughput rate up to time 5.0 sec is 97 kb/s. This is the throughput when the network is not under attack. At time 6.05, the malicious node starts attacking the mac layer of intermediate nodes 23 and 35. After this time the throughput falls drops rapidly to 33 kb/s as can be seen in the graph.

The simulation results show that this cross layer attack although aimed at affecting the MAC layer of the nodes, affects the TCP flow and there is a sudden fall in throughput rate (about 40%).

3.4 Conclusion

In this thesis, we have identified the Stasis Trap Attack in Cognitive Radio networks. This attack employs a cross layer design where the point of attack is at the MAC layer but the impact of the attack is on TCP layer throughput by exploiting the TCP congestion control mechanism in Cognitive Radio. This is a difficult attack to detect as the attack is target at one layer, but the effects are manifest at a higher layer.

CHAPTER IV

DEFENSE ON STASIS TRAP ATTACK BASED ON KEY PRE DISTRIBUTION

In this section, we process a novel deterministic pre distribution algorithm using the Chinese Remainder Theorem (CRT) [11] as a defense mechanism against the stasis attack.

4.1 Overview

An analysis of recently proposed MAC protocols reveals that they lack MAC layer authentication. In IEEE 802.22, which is a single hop network, there is a security sub-layer that provides confidentiality and authentication to MAC frames. The security sub-layer thwarts MAC-layer DOS (Denial of Service) attacks by preventing the modification of MAC frames. The security sub-layer employs an authenticated client/server key management protocol in which the base station acts as the trusted server. Unfortunately, such a protocol cannot be implemented in a multi-hop CR network since there is no trusted entity to act as a server. Without an authentication mechanism, adversaries can forge MAC control frames to launch these type of attacks.

Our aim is to provide security to the MAC layer by using a deterministic key pre distribution algorithm. The key distribution is such that, a pool of symmetric keys is chosen and a subset of the pool (key chain) is distributed to each node. If any two nodes want to communicate with each other, they search their key chain to see if they share a

common key. If they don't have any key in common, then they check with the neighboring nodes to see if they have a node which shares a common key individually with each of these nodes. This process continues till they find a key path through which they can communicate. For example, consider four nodes A, B, C, D and say, A and D want to communicate and have no keys in common. These two nodes check with the neighboring nodes (B, C) to see if they have any keys in common. If they find any, they communicate with that node. Here, say A and C have a common key and B and D have a common key and C and B also have a common key. Then, they communicate through the key path A -- C -- B -- D.

4.2 Key pre-distribution phase:

1) Parameter Selection:

We select the network size N

Next select the relative prime numbers, such that $N \leq M$, where $M = m_1 m_2 m_3 \ldots m_n$

2) Key Pool Arrangement:

The keys present in the key pool will be represented by using relative prime numbers. (KP_x -> Key Pool for all the relative prime numbers). The key pair is represented by (a_i, b_i) where a_i - is the identifier of the node and b_i - is the key value generated using Chinese remainder theorem

KP_0- (0, 0), (0, 1), (0, 2)… (0, m_1-1)

KP_1- (1, 0), (1, 1), (1, 2)… (1, m_2-1)

KP_2- (2, 0), (2, 1), (2, 2)… (2, m_3-1)

.

.

.

KP_{n-1}- (n-1, 0), (n-1, 1), (n-1, 2)… (n-1, m_n-1)

3) Key Chain Generation:

Key chain is a subset of keys chosen from the key pool. The key chains are generated by finding out the key combinations using the Chinese remainder theorem. The set of node identifiers is $A \varepsilon \{0 \text{ to } (N\text{-}1)\}$

Algorithm for key distribution:

- N number of nodes in the network and each node requires keys for communication.
- Choose Relative prime numbers (RPN) that satisfy the condition $M \geq N$, where $M = m_1 * m_2 * m_3 \ldots m_n$ and $m_1, m_2, m_3, \ldots m_n$ are relative prime numbers.
- The key pair is represented by (a_i, b_i) where a_i - is the identifier of the node and b_i - is the key value generated using Chinese remainder theorem.
- Assume Identifier $a_i = i$. Key value 'b_i' is calculated by using $b_i = A$ **mod** m_i where A is the unique ID of each node. m_i is the relative prime number chosen and b_i is the key value generated for the specific node.
- The pair wise symmetric keys are chosen from the key pool and are distributed to the nodes prior to network deployment by the key pre distribution mechanism.

- ➢ They communicate through a secure path on which every pair of neighboring nodes share a key.
- ➢ **Shared key discovery phase:** Source node determines the common key shared with the neighboring nodes from their identifiers.
- ➢ For example, for communication between nodes 3 and 7, the nodes check for common keys between them by using the unique ID of the nodes.
- ➢ If they don't share a common key, they communicate using the neighboring nodes as the intermediate nodes and have a secure communication as explained in Section 4.1

For example, consider the network size be 40. We choose relative prime numbers m_i where $M=m_1m_2\ m_3...m_n$. Let take 3 RPN (Relatively Prime Number) as m_0= 2, m_1= 3, m_2= 7 where M=42 > 40=N. So the condition is satisfied.

Key Pool:

KP_0: (0, 0), (0, 1)

KP_1: (1, 0), (1, 1), (1, 2)

KP_2: (2, 0), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6)

Key Chain Generation:

Key Chain (2, 3, 7): we get the result of $a_i = A$ **mod** m_i

So, the result becomes $a_0= A$ **mod** 2, $a_1=A$ **mod** 3, $a_2=A$ **mod** 7;

A	a_0	a_1	a_2
0	(0, 0)	(1, 0)	(2, 0)
1	(0, 1)	(1, 1)	(2, 1)
2	(0, 0)	(1, 2)	(2, 2)
3	(0, 1)	(1, 0)	(2, 3)
4	(0, 0)	(1, 1)	(2, 4)
5	(0, 1)	(1, 2)	(2, 5)
6	(0, 0)	(1, 0)	(2, 6)
7	(0, 1)	(1, 1)	(2, 0)
8	(0, 0)	(1, 2)	(2, 1)
9	(0, 1)	(1, 0)	(2, 2)
10	(0, 0)	(1, 1)	(2, 3)
11	(0, 1)	(1, 2)	(2, 4)
12	(0, 0)	(1, 0)	(2, 5)
13	(0, 1)	(1, 1)	(2, 6)
14	(0, 0)	(1, 2)	(2, 0)
15	(0, 1)	(1, 0)	(2, 1)
16	(0, 0)	(1, 1)	(2, 2)
17	(0, 1)	(1, 2)	(2, 3)

18	(0, 0)	(1, 0)	(2, 4)
19	(0, 1)	(1, 1)	(2, 5)
20	(0, 0)	(1, 2)	(2, 6)
21	(0, 1)	(1, 0)	(2, 0)
22	(0, 0)	(1, 1)	(2, 1)
23	(0, 1)	(1, 2)	(2, 2)
24	(0, 0)	(1, 0)	(2, 3)
25	(0, 1)	(1, 1)	(2, 4)
… … …	… … …	… … …	… … …
36	(0, 0)	(1, 0)	(2, 1)
37	(0, 1)	(1, 1)	(2, 2)
38	(0, 0)	(1, 2)	(2, 3)
39	(0, 1)	(1, 0)	(2, 4)
40	(0, 0)	(1, 1)	(2, 5)
41	(0, 1)	(1, 2)	(2, 6)

Table 1: Key Chain's distributed to each Node

4.3 key Pre Distribution in CR Network:

In the multi-hop CR MAC protocol, an adversary saturates the common control channel by transmitting spurious MAC control frames. In MAC layer, the Distributed channel negotiation is carried out with FCL (free channel list) and SEL (selection) frames. Here an attacker might send these frames continuously to saturate the channel.

To defend against such an attack, we introduce a novel architecture based on deterministic key pre distribution to the cognitive radio network. Here we distribute the keys using the above algorithm to all the nodes.

The channel availability is defined as the probability that a channel is accessible to a SU after sensing. In Cognitive Radio ad hoc networks, a SU can sense a number of available channels before accessing them. But as they are sparsely located and PU activities vary with location, it is likely that a channel available to an SU at one location might not be available to a SU at another location. Therefore channel availability is not common throughout the network.

Usually the channel availability is uncommon in MAC protocols. Therefore, the probability of a channel being common to nodes is comparatively small. Proposed new MAC protocol nodes do not require any Common Control Channel for exchanging the data [13].

The idea behind the proposed protocol is to have little network access delay and waiting

time. That is, communication pairs, as many as possible, should be able to start transmission simultaneously. For transmitting early, nodes should get a chance to reserve a channel as early as possible.

Here, we make use of two different channel lists, namely [13]

- The sorted channel list (SCL), which is a global list of all the channels in the network, sorted such that the first channel is most common and the last channel is the least common to all member nodes.
- The common channel list (CCL), which is a local list of all the channels common to a given communication pair, sorted in the reverse order.

For example, let the channel list of nodes N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, N_9 and N_{10} be

N_1: C3 C4

N_2: C2 C3 C4

N_3: C2 C3 C4

N_4: C2 C5

N_5: C2 C3 C4 C5

N_6: C1 C3 C4

N_7: C1 C4 C5

N_8: C1 C2 C3 C4

N_9: C1 C2 C4

N_{10}: C2 C5

SCL would be {C4, C2, C3, C5, C1}. The common channel list will be known to the channels common to a given communication pair. We are going to distribute keys for the above example. The network size (N) is 10 and assume 2 RPNs m_0= 2, m_1= 7 where M = 14 > 10. As explained before, based on the key pre-distribution algorithm, the following keys are distributed as follows:

Key Pool:

KP_0: (0, 0), (0, 1)

KP_1: (1, 0), (1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6)

Key Chain Generation:

Key Chain (2, 3, 7): we get the result of $a_i = A$ **mod** m_i

So, the result becomes $a_0 = A$ **mod** 2, $a_1 = A$ **mod** 3, $a_2 = A$ **mod** 7;

A	a_0	a_1	a_2
$N_1 1$	(0,1)	(1,1)	(2,1)
$N_2 2$	(0,0)	(1,2)	(2,2)
$N_3 3$	(0,1)	(1,0)	(2,3)
$N_4 4$	(0,0)	(1,1)	(2,4)
N_5 5	(0,1)	(1,2)	(2,5)
N_6 6	(0,0)	(1,0)	(2,6)
N_7 7	(0,1)	(1,1)	(2,0)
N_8 8	(0,0)	(1,2)	(2,1)
N_9 9	(0,1)	(1,0)	(2,2)
N_{10} 10	(0,0)	(1,1)	(2,3)

Table 2: Generating keys for above example

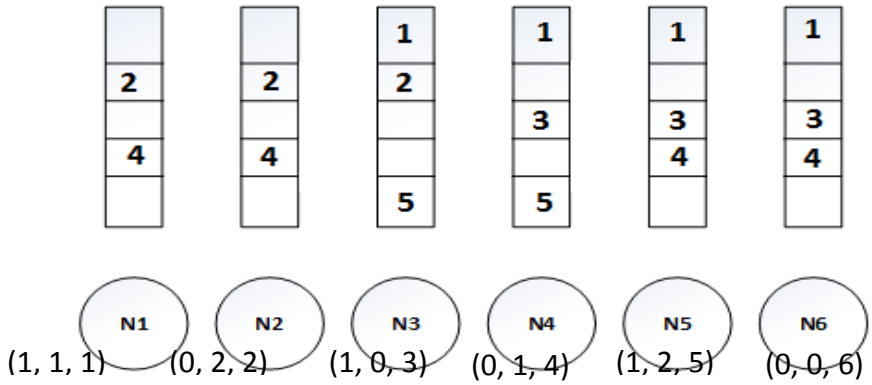

Figure 15: Common Channel List in the CR Nodes.

The above figure shows nodes with the available channels (listed in the rectangular box) and the keys (in brackets) at each node. We shall now discuss some cases, where the source node N1 wants to communicate with node N6.

Case 1: Share a key and have a common channel

Here N1 and N6 have a common channel 4 and both nodes have a common key 0 according to the above table 2. Therefore they can communicate with each other directly based on the algorithm discussed in 4.2

Case 2: Have a common channel but don't share a key

In this case if N1 and N6 have a common channel 4 but they don't share a common key. Let us assume N1 and N5 have a common key and similarly N5 and N6 share a key. Here N5 acts as an intermediate node and there will be successful communication between N1 -> N5 -> N6 through channel 4.

Case 3: If they don't have a common channel

If the source and destination don't have a common channel, then the source node looks for the neighbor nodes which have a common channel and a common key. In the above diagram if channel 4 is not available, then a PU is using it. Then N1 tries to communicate with node N3 using another channel, namely, channel 2. And N3 communicates with N6 using channel 1. Therefore there is successful communication between N1 -> N3 using channel 2 and N3 -> N6 using channel 1.

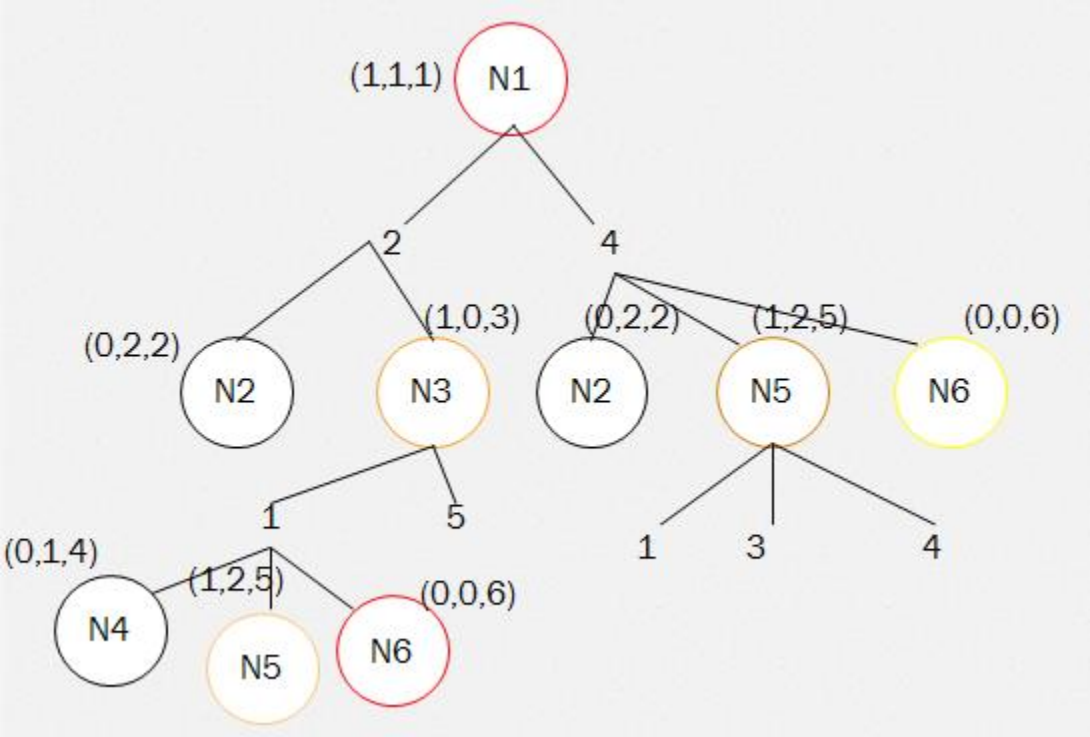

Figure 16: No common channel between N1 and N6

Denotations:

- Red Circle- Source and Destination nodes
- Black Circle – Node with a common channel but no common key with its parent node
- Orange Circle- Node with a common Key with its parent node.
- Yellow Circle- Destination Node with no common key.
- Edge represents nodes within communication range.
- Number in a circle represents node id.
- Individual number - available channels shared with parent node.
- Triplet (a, b, c) – Keys of a node (see Table 2)

Here, Node *N1* is trying to communicate with node *N6*. Firstly, the keys are pre-distributed to every Node (see table 2). *N1* looks for the Nodes in the available channel list to communicate and checks for common keys between them. *N1* and *N6* have a common channel 4 but cannot communicate as they don't have a common key. Hence *N1* looks for intermediate nodes through which it can communicate to *N6*.Here, it communicates with *N3* and *N5* through channel 2 and 4 with common key 1. Now *N3* tries to do the same and communicates with the nodes in the available channels and a common key. Here, N3 communicates with destination node N6 using channel 1 with key 0. Thus, the communication has taken place between *N1* and *N6* through *N3*.

4.4 Algorithm for generating a path between two nodes

Input C<List>=Φ [List is null]

Algorithm

N_S ← Source Node, N_D ← Destination Node

repeat

C_1<1.. n> [Channel list of the source node]

for i= 1 to n

N_J<1.. m> [Common Nodes under channel C_i]

for j = 1 to m

if (N_S (Key) == N_J (Key)) [Check for the common keys]

if ($\mathbf{N_J} == \mathbf{N_D}$) [Check for the Destination node]

then exit

else C<list>.add C_J<list> [Else add the intermediate node channels to C<list>]

C_1 = C<list>

until K=0 [Until it exits the loop]

Output: Path for the destination node

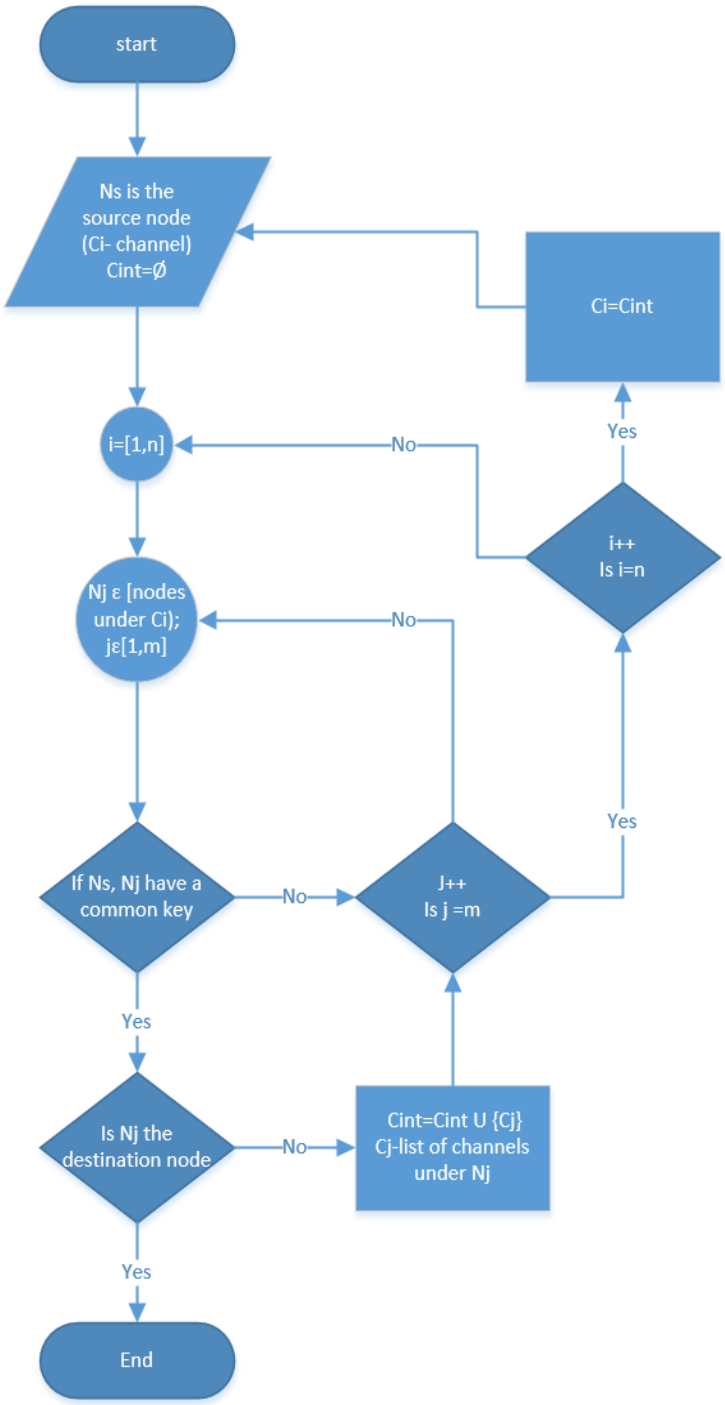

Figure 17: Pictorial representation for communication between source and destination

4.5 Simulation Results

Analysis for CRT – Key Pre Distribution

Key connectivity is a measure of the probability of key-sharing between two or more nodes. That is, it is a measure of the number of pairs of nodes that have at least one key common between them out of the total number of possible pairs of nodes. As the size of the key chain increases, the probability of key sharing between the nodes will increase. Hence the key connectivity increases. Say there are 'N' numbers of nodes in the network. So the total numbers of pairs of possible nodes are N (N-1)/2.

The number of pairs of nodes having at least one key (N_{KCS}) can be derived as follows. Let us consider we have $m_0m_1m_2m_3$. N_{KCS} is [Number of key connectivity sharing key in MSB (0^{th}) position] + [Number of key connectivity sharing key in 1^{st} position - Number of key connectivity sharing key in both 1^{st} and 0^{th} position] + [Number of key connectivity sharing key in 2^{nd} position ─ Number of key connectivity sharing key in (2, 0) position ─ Number of key connectivity sharing key in (2, 1) position + Number of key connectivity sharing key in (2,1,0) position] + [Number of key connectivity sharing key in 3^{rd} position ─ Number of key connectivity sharing key in (3,0) position ─ Number of key connectivity sharing key in (3,1) position ─ Number of key connectivity sharing key in (3,2) position + Number of key connectivity sharing key in (3,0,1) position + Number of key connectivity sharing key in (3,0,2) position + Number of key connectivity sharing

key in (3,1,2) position].

So $N_{KCS} = m_0m_1m_2m_3\ (m_1m_2m_3-1)/2 + m_0m_1m_2m_3\ (m_0m_2m_3-1)/2 - m_0m_1m_2m_3\ (m_2m_3-1)/2 + m_0m_1m_2m_3\ (m_0m_1m_3-1)/2 - m_0m_1m_2m_3\ (m_1m_3-1)/2 - (m_0m_1m_2m_3\ (m_0m_3-1)/2) - m_0m_1m_2m_3\ (m3-1)/2 + m_0m_1m_2m_3\ (m_0m_1m_2-1)/2 - m_0m_1m_2m_3\ (m_1m_2-1)/2 - (m_0m_1m_2m_3\ (m_0m_2-1)/2) - m_0m_1m_2m_3\ (m_2-1)/2 - (m_0m_1m_2m_3\ (m_0m_1-1)/2) - m_0m_1m_2m_3\ (m_1-1)/2 - m_0m_1m_2m_3\ (m_0-1)/2.$

Hence the number of pairs of nodes having at least one key is:

$N_{KCS} = \sum_{i=1}^{(n+1)cn} M\text{ni} - \sum_{i=1}^{(n+1)cn-1} M(\text{n}-1)\text{i} + \cdots + (-1)n - j \sum_{i=1}^{(n+1)cj} Mji + \cdots + (-1)n - 1 \sum_{i=1}^{(n+1)c1} M1\text{i} - (n+1)Cn + \ldots + (-1)n - i - 1(n+1)ci + \cdots (-1)n - 2(n+1)c1.$

Java code for generating keys for all the nodes in the network was written for simulation. The network size, key chain size and the relative prime numbers that are used in generating the keys for all the nodes in the network are input. The nodes in the network are static. The formula calculates key connectivity. The following are a few scenarios showing how key connectivity changes by varying different parameters.

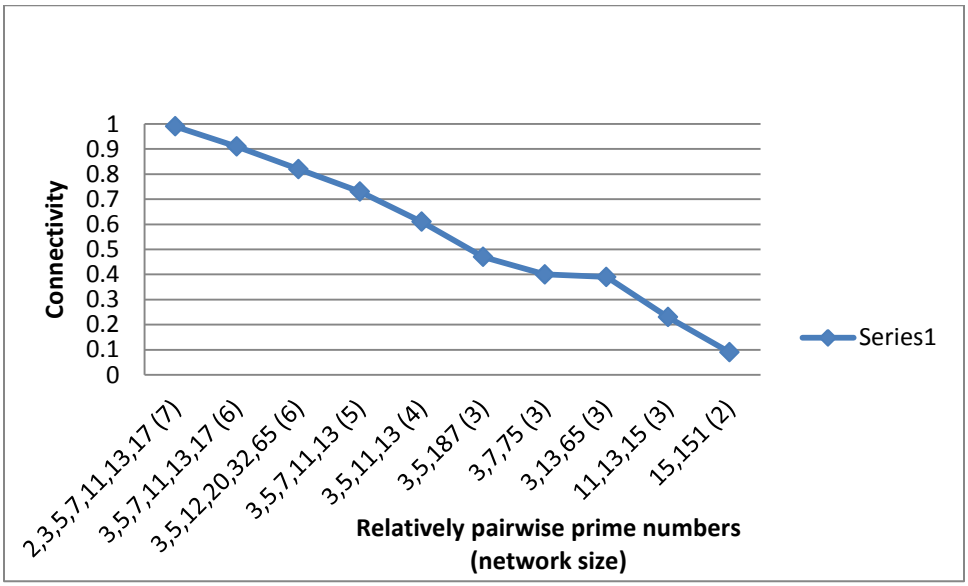

Figure 18: Key Connectivity with different set of RPN numbers

The above figure shows key connectivity for a network size of 2000 using different combinations of PRP (Pairwise Relatively Prime numbers) with different key chain sizes. From the graph, a higher connectivity is observed with the set of PRPs that are prime. For example consider PRP numbers set1, (2, 3, 5, 7, 11, 13, 17). All of them are prime numbers. Consider another set3 (3, 5, 12, 20, 32, 65) and here some are not prime. Connectivity for the set1 is 0.1, but for set2 connectivity is 0.82. So connectivity can be increased by selecting PRP numbers which are primes themselves.

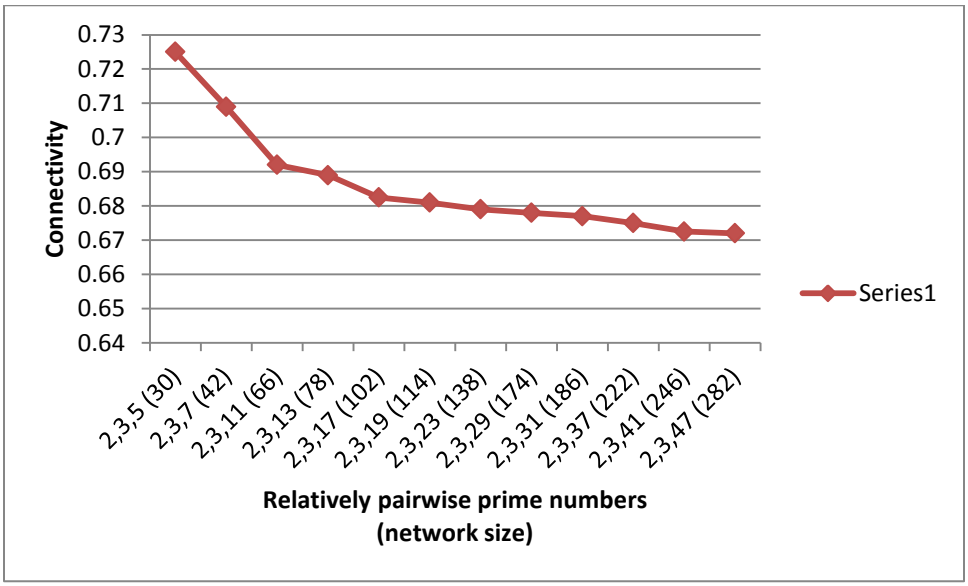

Figure 19: Key Connectivity for various network sizes with constant keychain size

The above figure shows the key connectivity for various network sizes using different combinations of PRP numbers which are prime with constant key chain size of three. In this scenario, we observed a higher connectivity for the smallest PRP numbers combinations, i.e. a smaller network size.

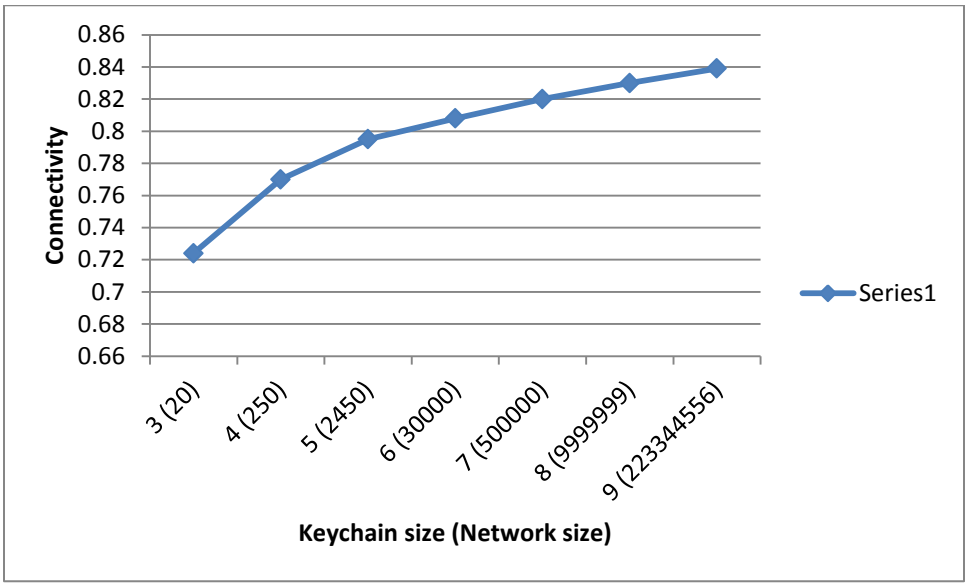

Figure 20: Key Connectivity for various network sizes with different key chain sizes

Key connectivity using different key chain sizes for different network sizes is assessed by selecting PRP numbers as smallest continuous combinations of prime. It is observed from the graph that by increasing key chain size with network size, connectivity also increases.

Analysis on Key pre Distribution in a CR Network

The main task is to safely distribute the shared keys to the node. The key pre distribution is such that, a pool of symmetric keys is chosen and a subset of the pool (key chain) is distributed to each node. If any two nodes want to communicate with each other, they search their key chain to see if they share a common key. If they don't have any key in common, then they check with the neighboring nodes to see if they have a node which shares a common key individually with each of these nodes. This process continues till

they find a key path through which they can communicate.

Our simulation uses ns2.34 (network simulator) [15], we investigated the effect of stasis trap attack on network performance. Node mobility was not considered in the simulation. The network topology consists of 50 nodes. Choosing 4 relative prime numbers (2, 3, 5, 7). In cognitive radio the data is transmitted through the channels, after the channel allocation only it transmits data. For simulation purpose, we have chosen common channel among the nodes for communication. The source node communicates with the neighbor nodes through common key to reach the destination. Here source node 20 communicates with node 21 through common key (0), node 21 communicate with node 22 through key (1), node 22 communicates with node 23 through key (1), node 23 communicates with node 24 through key (3) and node 24 communicates with destination node 45 through key (0). At a certain time attacker node 29 attacks the Mac layer of data transmitting node 23.

When an attacker tries to communicate with an intermediate node, the node cannot send ACKs to the source node through its neighboring node before its timeout. Hence the source node knows what node is under attack and tries to take an alternative path to the destination that avoids the node under attack. The alternative path is chosen based on a Tree-based algorithm (see section 4.4). It finds an alternative shortest path such that the intermediate node under attack is not in the path. If the attack takes place in the new path also, another path to communicate is determined.

Node-Id	keys	common-key
20	0,2,0,6	
21	1,0,1,0	0
22	0,1,2,1	1
23	1,2,3,2	1
24	0,0,4,3	3
45	1,0,0,3	0
20	0,2,0,6	
14	0,2,4,0	0
15	1,0,0,1	0
16	0,1,1,2	1
17	1,2,2,3	1
18	0,0,3,4	3
44	0,2,4,2	0
45	1,0,0,3	0

Table 3: Node-Id with their keys and common keys

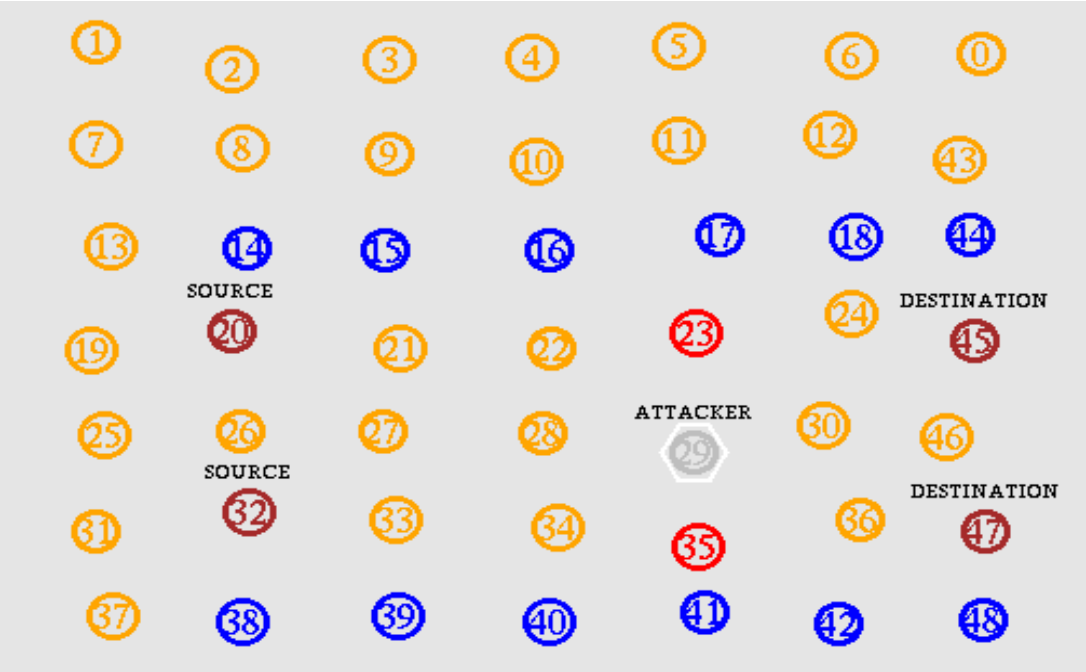

Figure 21: Alternative path when an intermediate node in the TCP flow is attacked

The alternative path goes through nodes 20, 14, 15, 16, 17, 18, 44 and 45. Here source node 20 communicates with node 14 through common key (0), node 14 communicates with node 15 through key (0), node 15 communicates with node 16 through key (1), node 16 communicates with node 17 through key (1), node 17 communicates with node 18 through key (3), node 18 communicates with node 44 through key (0) and node 44 communicates with destination node 45 through key (0) [see figure 21].

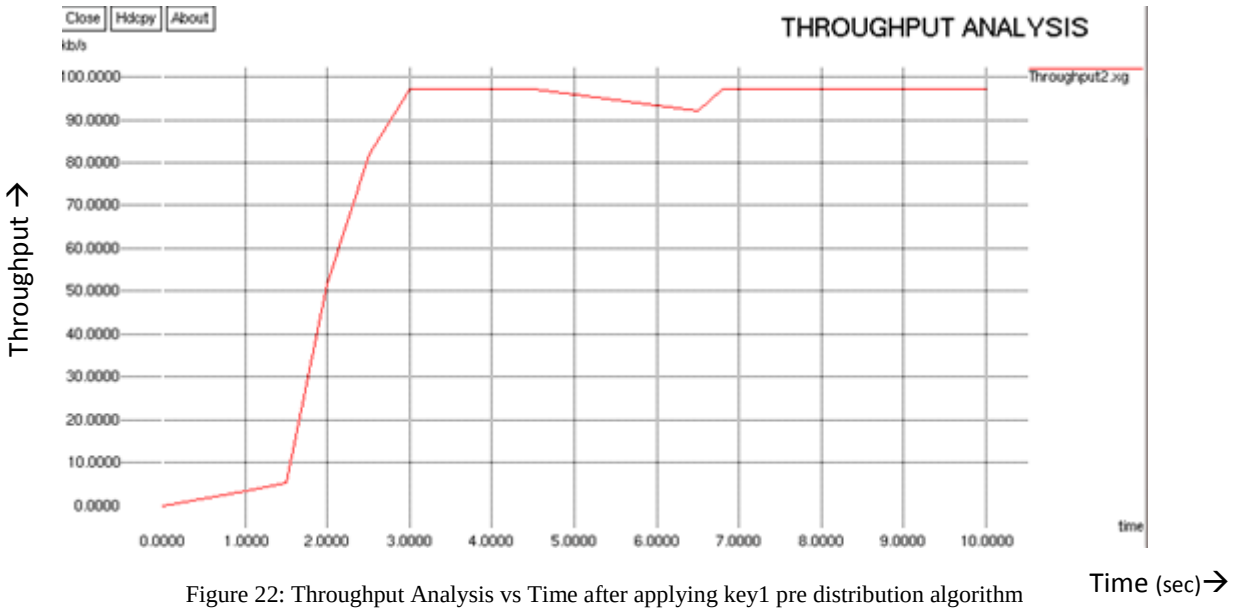

Figure 22: Throughput Analysis vs Time after applying key1 pre distribution algorithm

The graph shows that the throughput is about 97 kb/s until 6.4 sec, at this point the attacker attacks the mac layer of the intermediate node 23, which results in a slight drop in throughput rate. As soon as the attack begins the source node takes an alternate path to the destination through common keys and channels. As the graph shows, the throughput rate returns to 97kb/sec.

CHAPTER V

CONCLUSIONS

In this thesis, we have identified a multi-layer attack on CRNs where the attack is targeted at the MAC layer to cause channel saturation. The effect of the attack is seen at the TCP layer where throughput is substantially reduced. Simulation results show that the TCP performance was reduced due to the attack.

We have also proposed a defense against the multi-layer stasis trap attack, using a deterministic key pre-distribution scheme. The process of determining the keys or key chain is based on the Chinese remainder theorem. Simulation results show that even though the throughput was slightly reduced at the start of the attack, the throughput was restored to its pre-attack levels by finding an alternative path.

Future work would include more detailed analysis of the proposed framework. We can also identify other multi-layer attacks in cognitive radio network. The defense framework can be used for the effectiveness of other multi-layer attacks in CRNs.

REFERENCES

[1] Kaigui Bian, Jung-Min Park and Ruiliang Chen, "Stasis Trap: Cross-Layer Stealthy Attacks in Wireless Ad Hoc Networks". *Proceedings of IEEE Conference on Global Telecommunications*, GLOBECOM'06, Pages 1 – 5, 2006.

[2] Dilip Sarkar and Harendra Narayan, "Transport Layer Protocols for Cognitive Networks". *Proceedings of IEEE Conference on Computer Communications Workshops*, INFOCOM, Pages 1 – 6, 2010.

[3] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran and Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey", *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Volume 50, Issue 13, Pages 2127 – 2159, 2006.

[4] Kaigui Bian and Jung-Min Park, "MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks". *Proceedings of US-Korea Conference on Science, Technology and Entrepreneurship*, Pages 1 – 8, August 2006.

[5] Yan Zhang and Loukas Lazos. "Vulnerabilities of Cognitive Radio MAC Protocols and Countermeasures". *IEEE Transactions on Network*, Volume 27, Issue 3, Pages 40 – 45, 2013.

[6] Wenkai Wang and Yan (Lindsay) Sun, Husheng Li and Zhu Han. "Cross-Layer Attack and Defense in Cognitive Radio Networks". *Proceedings of IEEE Conference on Global Telecommunications*, GLOBECOM'10, Pages 1 - 6, 2010.

[7] Wassim El-Hajj, Haidar Safa and Mohsen Guizani, "Survey of Security Issues in Cognitive Radio Networks". *Transaction on Internet Technology*, volume 12, Pages 1 – 18, 2011.

[8] Mansi Thoppian, S. Venkatesan, Ravi Prakash and R. Chandrasekaran, "MAC-layer scheduling in Cognitive Radio based Multi-hop Wireless Networks". *Proceedings of IEEE Conference on World of Wireless, Mobile and Multimedia Networks*, Pages 192 – 202, 2006.

[9] Alexandros G. Fragkiadakis, Elias Z. Tragos and Ioannis G.Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks". *IEEE Transaction on Communications Surveys & Tutorials*, Volume 15, Issue 1, Pages 428 – 445, 2012.

[10] Ian F. Akyildiz, Brandon F.Lo and Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks". *Physical communication*, Volume 4, Pages 40 – 62, 2011.

[11] T. Kavitha, S. Jenifa Subha Priya and D. Sridharan, "Design of Deterministic Key pre distribution using number theory". *Proceedings of IEEE Conference on Electronics Computer Technology*, Pages 134 – 137, 2011.

[12] Matteo Cesana, Francesca Cuomo and Eylem Ekici. "Routing in cognitive radio networks: Challenges and solutions". *Ad Hoc Networks*. Volume 9, Issue 3, Pages 228 – 248, 2011.

[13] Sunil K Timalsina, Sangman Moh, Ilyong Chung, Moonsoo Kang. “A concurrent access MAC protocol for cognitive radio ad hoc networks without common control channel”. *Advances in Signal Processing*. Volume 69, Pages 1 – 13, 2013.

[14] Yogesh R Kondareddy and Prathima Agrawal. “Synchronized MAC Protocol for Multi-hop Cognitive Radio Networks”. *IEEE International Conference on Communications*, Pages 3198 – 3202, 2008.

[15] Source forge, www.sourceforge.net/projects/nsnam/files/ns-2, Date of last access: 13th April, 2014.

VITA

Dileep Nagireddygari

Candidate for the Degree of

Master of Science

Thesis: STASIS TRAP: CROSS LAYER ATTACK & ITS DEFENSE IN COGNITIVE RADIO NETWORKS

Major Field: Computer Science

Biographical:

Education:

Completed the requirements for the Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma in May, 2013.

Completed the requirements for the Bachelor of Science in Information Technology at VIT University, Vellore, India in May, 2010.

Experience:

Graduate Teaching Assistant, Department of Computer Science, Oklahoma State University: Stillwater, OK Aug 2013 – May 2014

Graded assignments and maintained confidential student information.
Helped students in the lab for JAVA course

Graduate Research Assistant, Department of Computer Science, Oklahoma State University: Stillwater, OK Mar 2013 – Aug 2013

Worked on the attacks & security on cognitive radio networks.
Written a paper on the cross layer attack in Cognitive radio networks.

Systems Engineer, Infosys Technologies Ltd, Hyderabad, India Jun 2010 – Jun 2012

Completed training in java web application development using JSPs and Servlets.
Worked on design, development, implementation and support of web-based distributed applications
Worked in a team to develop and support a web application for an E-commerce company.